DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

EMERGENCY ORDINANCE 104/2021

on establishing the National Cyber Security Directorate

Friday 24 September 2021

The challenges, risks and security threats in cyberspace have intensified in recent years, and cyber security has become a requirement involving integrated, comprehensive approaches, adoption of new and permanent cyber security strategies, significant financial investments, and rapid and ambitious organizational adaptations,

given that cyber threats do not have a clear national address of a sender, are not blocked at state borders, have a deep asymmetric character, because, with relatively limited resources, an individual or a group of individuals, affiliated or not with governmental structures, can generate incidents with significant disruptive effects with a destabilizing impact at the state or economic sector level,

considering that both Member States of the European Union and many other states, including NATO, have recognized, in 2016, the cyberspace as a space for confrontation and operational domain, along with terrestrial, air, space and maritime domains,

considering that in order to ensure a high level of security of the networks and information systems supporting the provision of essential services in Romania as an EU Member State, the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems in the Union is vital for economic and social activities and, in particular, for the functioning of the internal market,

following the evaluation done by the European Commission regarding the activity of implementation of Directive (EU) 2016/1148 in Romania, where delays and non-conformities in the national approach were noted,

following EU Regulation 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cyber Security Research, Technology and Industrial Competence Centre and the National Coordination Centres Network hosted by Romania,

regarding Romania's obligations under the new European Union's Cybersecurity Strategy for the Digital Decade, based on the Joint Communication to the European Parliament and the Council JOIN (2020) 18 final of 16 December 2020,

motivated by the fact that, first, the digital transformation exposes the state, the society, the economy, and the citizens to asymmetric threats and cyber-attacks defined by low costs and by the fact that the attacker has the initial advantages,

motivated by the need to develop response capabilities that must evolve at the same time with the cyber-attacks, both by means of prevention and specialized reaction and intervention, highly prepared and adapted to new types of cyber-attacks,

motivated by the need to increase the cyber resilience, in the context of increasing frequency and complexity of cyber-attacks against infrastructures supporting essential services for the Romanian society and economy, which can lead to extraordinary situations of blocking vital infrastructures in a wide range of public and private domains,

aiming at the management of cyber threats, to the extent that the associated risks are very real and significant, to prevent insecurity, economic losses, or the impact on activities,

moreover, for a more active presence of Romania on the world map of the states with high reaction and intervention capabilities and, finally, for Romania to become a nexus / node of regional / global cyber influence and implicitly to the consolidation of the international image of country,

aiming for the new institution to become an international-level institution that firmly positions Romania as a recognized leader in cyber security,

considering the above as the premises of an emergency and extraordinary situation whose regulation cannot be postponed,

Pursuant to article 115 paragraph (4) of the Romanian Constitution, republished,

The Government of Romania adopts this emergency ordinance.

Art. 1 Establishing the Directorate

(1) The National Cyber Security Directorate (Directoratul Național de Securitate Cibernetică) is established, hereinafter referred to as NCSD (DNSC), specialised body of the central public administration, under the authority of the Government and in the coordination of the Prime Minister, with legal personality, entirely financed from the state budget, through the budget of the General Secretary of the Government.

(2) The National Cyber Security and Incident Response Team - CERT-RO shall be abolished upon the entry into force of this emergency ordinance.

(3) On the date of entry into force of this emergency ordinance NCSD takes over the activities, attributions, and staff of the National Cyber Security Incident Response Team - CERT-RO, maintaining the salary rights held at the date of takeover.

(4) NCSD has its headquarters in Bucharest, Italiană Street, no. 22, district 2, in the property of the Romanian State and under the administration of CERT-RO, according to HG no.1005/2020 on the transmission of a building located in the public domain of the State under the administration of the Ministry of Transport, Infrastructure and Communications in the administration of the National Center for Response to Cyber Security Incidents – CERT-RO, with the destination of headquarters of CERT-RO, and for the modification of the Government Decision no. 494/2011 on establishing the National Centre for Response to the National Security Incidents – CERT-RO.

(5) NCSD has the quality of permanent member of the Cyber Security Operative Council (Consiliul Operativ de Securitate Cibernetică), hereinafter referred to as CSOC (COSC).

(6) NCSD has responsibilities regarding the cyber security of the national civilian cyberspace.

(7) NCSD has in its internal structure functional compartments as well as other structures under its subordination, without legal personality.

(8) NCSD establishes regional and county structures without legal personality.

Art. 2 Concepts, definitions, and terms

For the purposes of this emergency ordinance, the terms and expressions below have the following meanings:

a) **CSIRT** – cyber security incident response team - a specialized organizational entity that has the necessary capacity to prevent, analyse, identify, and respond to cyber incidents;

b) **the CSIRT community in Romania** – the set of CSIRT teams operating within the public authorities and institutions or other legal entities of public or private law in Romania and who relates with the National Cyber Security Directorate based on cooperation procedures and protocols;

c) **cyberspace** – the virtual environment, as defined in the Romania's Cybersecurity Strategy and the National Action Plan on the implementation of the National Cyber Security System, approved by Government Decision No. 271/2013;

d) **the national civilian cyberspace** – the national cyberspace that excludes the cyber infrastructures that are, according to the legal provisions, under the administration or responsibility of the institutions from the national defence system, public order, and national security, as well as those that use classified information;

e) **cyber security** – state of normalcy, as defined in the Romanian Cyber Security Strategy and the National Action Plan on the implementation of the National Cyber Security System, approved by Government Decision no. 271/2013;

f) **cyber threat** – any circumstance, event or potential action that could cause damage or disruption to networks and computer systems, as well as to users of such systems and other people, or which may have a different negative impact on them;

g) **preventive public services** – are those services offered by the National Cyber Security Directorate, which consist of:

1. notifications regarding events in the field;
2. notifications regarding newly identified threats at national and international level;
3. research and inform on technological innovations in the field;
4. performing, upon request, security audits and evaluations or penetration tests;
5. identification of vulnerabilities and provision of up to date reports regarding intrusion attempts and services to identify the sources of attacks, based on the information transmitted by the providers of electronic communications networks and services;
6. dissemination of cyber security information.

h) **reactive public services** – are those services offered by the National Cyber Security Directorate, which consist of:

1. alerts and warnings regarding the occurrence of pre-attack activities;
2. incident management at national level, in cooperation with other CSIRT teams;
3. dissemination of the results of the cyber security incident investigations, in compliance with the provisions of the cooperation agreements concluded with the partners of the National Cyber Security Directorate.

i) **public consulting services for the management of cyber security services** – are those services offered by the National Cyber Security Directorate, which consist of:

1. risk analysis applied locally and nationally regarding the cyber infrastructures of national interest;
2. planning to ensure continuous operation and disaster recovery;
3. certification of cyber security management and cyber incidents;
4. authorization of the CSIRT teams and certification of the information security auditors specifically for the field of security of the networks and information systems.

j) **early warning system and real-time information on cyber incidents** – the set of procedures and technical systems that have the role of identifying the preliminary conditions for the occurrence of cyber incidents and to warn in case of their occurrence. The system also includes data connections that will carry on information on cyber incidents identified by dedicated sensors, as well as statistical information on traffic values recorded in the network nodes of cyber infrastructures that provide public utility functionalities or provide services of the information society;

k) **cyber crisis** – a situation that represents a real threat or deterioration of a cyber infrastructure, likely to create damage to networks and computer systems that provide essential services, digital services, or services of national interest;

l) **cyber security product** – an element or group of elements that ensure the security of a network or an information system;

m) **cyber security service** – a service that ensures the confidentiality, integrity, availability, authenticity, non-repudiation of a network or computer system.

Art. 3 Responsibilities and principles

(1) The main responsibility of NCSD is to ensure the cyber security of the national civilian cyberspace, in collaboration with the competent institutions and authorities.

(2) NCSD is the competent authority at the national level for the national civilian cyberspace, including the management of risks and cyber incidents.

(3) While performing its role of national-level competent authority, NCSD liaises and cooperates with:

a) The Romanian Intelligence Service (Serviciul Român de Informaţii) – on ensuring cybersecurity of the national civil cyberspace, whose impairment affects national security.

b) The Ministry of National Defence (Ministerul Apărării Naționale) – on ensuring cybersecurity of the national civil cyberspace, whose impairment affects national security.

c) The Ministry of Internal Affairs (Ministerul Afacerilor Interne), the Foreign Intelligence Service (Serviciul de Informații Externe), the Special Telecommunications Service (Serviciul de Telecomunicaţii Speciale), and the Protection and Guard Service (Serviciul de Protecţie şi Pază) – on ensuring cybersecurity of the national civil cyberspace, whose impairment affects their field of activity and responsibility.

d) The Presidential Administration – on ensuring cybersecurity of the national civil cyberspace, whose impairment affects its field of activity and responsibility, as well as for those intended for the Supreme Council of National Defence (Consiliul Suprem de Apărare a Ţării), hereinafter referred to as SCND (CSAT), which are managed according to the decisions adopted by this, under the law.

(4) To fulfil its responsibilities, NCSD liaise and cooperates, accordingly, with:

a) public institutions mentioned in paragraph (3).

b) The National Authority for the Supervision of Personal Data Processing (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal), in case of incidents that result in breach of the security of personal data, in accordance with the law.

c) The National Authority for Administration and Regulation in Communications (Autoritatea Națională pentru Administrare și Reglementare în Comunicații), when the incidents result in affecting the security or the functioning of the public electronic communications networks or whenever managing an incident requires measures that fall within its area of activity and responsibility.

d) The Office of the National Register of State Secret Information (Oficiul Registrului National al Informațiilor Secrete de Stat), in case of cyber incidents and attacks on the information and communication systems that use classified information.

e) The Ministry of Foreign Affairs (Ministerul Afacerilor Externe), in case of incidents and cyber-attacks that affect Romania's foreign interests.

f) The criminal investigation bodies, in accordance with the law.

(5) To achieve the objectives and functions, NCSD applies the following principles:

a) **The legality principle** – both NCSD and the staff of the institution act in compliance with legal provisions in force and with the international treaties and conventions to which Romania is a party.

b) **The equality principle** – the beneficiaries of the activities carried out by NCSD will be treated equally, in a non-discriminatory manner, correlated with the obligation of NCSD of national authority to treat equally all beneficiaries, without discrimination, based on criteria mentioned by the applicable legislation.

c) **The transparency principle** – in the process of drafting normative acts, NCSD will inform and submit to public consultation and debate the draft acts and will provide the access of both legal and natural persons to data and information of public interest, according to the Law no. 544/2001 on free access to the information of public interest, with subsequent amendments and additions. At the same time, the stakeholders of NCSD have the right to obtain information from the institution, and the institution has the obligation to provide the required information ex officio or upon request, within the limits of the law.

d) **The proportionality principle** – the forms of activity of NCSD must be aligned with the national law and fulfil the public interest, as well as they must be balanced from the point of view of their effects on the natural and legal persons.

e) **The impartiality principle** – the NCSD staff perform their legal attributions without subjectivism, regardless of their own beliefs or interests.

f) **The continuity principle** – the activity of NCSD is performed with no interruptions, in compliance with the legal provisions.

g) **The technological neutrality principle** – in performing the specific activity of regulation, testing, and evaluation, NCSD does not favour a certain brand or technology and does not impose or discriminate in favour of the use of a certain type of technology.

h) **The international solidarity principle** – in relations with partners from European Union and other states or organisations NCSD promotes the cooperation between states to solve as efficiently as possible the cyber security global challenges.

i) **The synchronization principle** – the security measures and requirements enforced by NCSD will consider the evolution of the cyber security phenomenon at the European Union level.

j) **The principle of fulfilling the public interest** – NCSD, as well as the staff of the institution pursue the fulfilling of the public interest above the individual or group interest. The national public interest is above the local public interest.

k) **The awareness principle** – in its awareness activity towards individuals and legal entities, as well as citizens, NCSD presents new knowledge and information on vulnerabilities, risks, and cyber-attacks, in plain terms, using various methods to draw the attention of target groups.

(6) In fulfilling its functions, NCSD aims to achieve its objectives by taking reasonable measures, while respecting the principles mentioned in paragraph (5).

(7) The responsibilities of NCSD are without prejudice to the legislation in force regarding the national system of defence, public order and national security, the national critical infrastructures, and classified information.

Art. 4 Objectives

The main objectives of NCSD are:

a) To ensure the security, confidentiality, integrity, availability, resilience of the components of the national civilian cyberspace, in cooperation with the institutions that have competencies and responsibilities in the field.

b) To ensure the framework of strategies, policies, and regulations that support the implementation of the national vision in the field of cyber security.

c) To create the national framework for cooperation between public, private, education, and research institutions to ensure a realistic, common, and coherent vision and approach regarding the cyber security in Romania.

d) To create and operate a national collaboration platform that would allow the information exchange between constituents, state institutions, academia, and the private sector in the field of cyber security incidents, vulnerabilities, and crises.

e) To create the national certification framework in the field of cyber security, in cooperation with the institutions that have competencies and responsibilities in the field.

f) To create the national training framework in the field of cyber security, in cooperation with the institutions that have competencies and responsibilities in the field.

g) To promote and support internationally the national cyber security strategy.

h) To create the national framework for evaluation of the new technologies and of their impact on Romania's cyber security.

i) To develop capacity for attract financing to achieve the institutional objectives.

j) To elaborate and coordinate the cyber security crisis management plan at national level, in cooperation with the institutions that have competencies and responsibilities in the field of crisis management, as well as through cooperation with the other permanent members of CSOC.

Art. 5 Functions and responsibilities

In fulfilling the objectives, NCSD performs the following functions and responsibilities:

a) Strategy and planning

1. carries out the Government's policy in the field of cyber security and establishes at the national level the public strategies and policies in the field of cyber security.
2. ensures the development and dissemination of public policies for preventing and mitigating incidents within the cyber infrastructures of the national civilian cyberspace.
3. take part in the development of the national cyber security strategy in cooperation with the institutions from the National Defence, Public Order, and National Security System (Sistemul Național de Apărare, Ordine Publică și Securitate Națională), hereinafter referred to as NDPONSS, and coordinates its implementation, throughout monitoring of the actions taken and evaluation of the results.
4. develops and coordinates the application of the cyber security crisis management plan at the national level in peacetime, in cooperation with the institutions that have competencies and responsibilities in the field of crisis management.
5. develops and coordinates the implementation of the national training strategy in the field of cyber security, in cooperation with the institutions that have competencies and responsibilities in the field.
6. develops and coordinates the implementation of the national strategy of cooperation between public, private, education, and research institutions to ensure a realistic, common, and coherent vision and approach regarding the cyber security of Romania, also from the viewpoint of training and retaining in Romania of the human resource.
7. drafts and submits to the Government of Romania proposals for modification of the legislative framework in the field of cyber security.
8. provides support to public authorities in developing and implementing national sectoral strategies, which also include cyber security components.
9. supports the participation of Romanian state institutions and of other stakeholders in national and international cyber security projects, to fulfil the national cyber security strategy objectives.

b) The function of national competent authority for regulation, supervision, and control - ensures regulation and management of the Romania’s cyber security and national civilian cyberspace, as follows:

1. monitors the implementation of national and sectoral cyber security strategy and policies.

2. develops the regulatory and institutional cyber security framework, initiates and respectively issues opinions on draft acts in its field of competence, and further submits these for approval, in accordance with the law.
3. exercises the responsibilities established by Law no. 362/2018 on ensuring a high common level of network and information system security, as amended and supplemented.
4. develops regulations, norms, requirements, guides, and recommendations in the field of competence, which are approved by decision of the Director of NCSD and published, as appropriate, in the Official Gazette of Romania or on the website.
5. fulfils the responsibilities of national authority for hosting services providers, cloud services, eID services, trust services for e-transactions and content distribution network providers.
6. establishes the standards and regulations in the field of cyber security at national level, except for those domains mentioned in art. 20 paragraph (1), which become mandatory once published in the Official Gazette of Romania, Part I, and verifies their implementation through control actions.
7. manages and administers records regarding natural and legal persons under the provisions of the normative acts that regulate the field of cyber security, according to the responsibilities of the institution.

c) The function of national CSIRT

1. ensures the coordination of activities at national level of detection, protection, and response to cyber-attacks, as well as the conduct of monitoring, identification, analysis, investigation, and response to cyber security incidents, through the national CSIRT team, for cyber infrastructures in its field of competence, as defined by NCSD's internal rules.
2. performs the role and responsibilities of a national CSIRT as established by Law no. 362/2018.
3. coordinates the response for national level cyber security incidents for its field of competence.
4. monitors, identifies, analyses and responds to cyber security threats in the national civilian cyberspace.
5. investigates cyber incidents that target or use the national civilian cyberspace, in accordance with its legal competencies, by using appropriate technical methods that include analysis of network metadata as provided to NCSD by its respective owners.
6. assesses cyber security risks at national level and issues warnings, newsletters, and forecasts.
7. identifies and analyses threats, also in cooperation with the public, private and academic stakeholders, to implement a high level of cyber security.
8. carries out specific technical activities to identify vulnerabilities of websites with content in Romanian language and issues security warnings, as appropriate.
9. develops systems and tools for identification, analysis and forecast of cyber incidents, based on which it establishes the impact at national and cross-border level of incidents and notifies the relevant authorities at national level, as well as similar authorities from other potentially affected states. In this regard, NCSD cooperates with the institutions from national defence system, public order, and national security, as well as with private and academic stakeholders.
10. in accordance with the law, performs the collection, the analysis and exchange of information on cyber security risks and vulnerabilities of computer networks and systems, as well as of cyber security products and services.
11. provides public preventive, reactive and consulting services for cyber security management.
12. creates, manages, and coordinates the National Platform for Reporting Cyber Security Incidents (Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică), hereinafter referred to as NPRCSI (PNRISC).

d) The function of governmental CSIRT

1. monitors the implementation of cyber security measures at the level of Romanian Government institutions, in collaboration and coordination with state institutions that have competencies and responsibilities in the field.
2. supports the state institutions that have competences and responsibilities in the field, in performing their responsibilities related to cyber security.

e) The function of coordination, implementation, guidance, and support of the sectoral CSIRTs

1. performs or contributes to the function of sectoral CSIRT for all sectors specified by Law no. 362/2018, with subsequent amendments and additions, in collaboration and coordination with the state bodies that have competencies and responsibilities in the field and with the regulatory authorities from the involved sectors.
2. in cooperation with the institutions or organisations that coordinate and/or regulate fields of activity that may be affected by cyber security incidents, it develops sectoral CSIRT teams or participate in enhancing the capabilities of teams set up at sectoral, sub-sectoral, or institutions or organisations level.

f) The function of the cyber security incident response team for IT products and services used in the government sector

1. performs the identification, assessment, and management of risks associated with cyber security vulnerabilities of IT products, solutions, components, and/or services of the government sector.
2. provides the necessary infrastructure and processes for receiving, investigating, and reporting publicly or to state bodies with competencies and responsibilities in the field, concerning the information on cyber security vulnerabilities of products, solutions, components, and/or services of the government sector.

g) Alerting, prevention, awareness, and training function

1. informs and provides training at national level for the population as well as for all entities that are part of the national civilian cyberspace, also for economic operators from the sectors as defined in the Law no. 362/2018 with subsequent amendments and additions and from the public sector, regarding the security risks in the civilian cyberspace.
2. promotes the development of adequate behaviour in the national civilian cyberspace for the natural and legal persons through awareness concerning the consequences of the cyber-attacks and of the manner of reporting them.
3. issues notifications on the obligations as administrator, provider or user of computer networks and systems, on the reply towards possible cyber-attacks, on the awareness of citizens and public and private institutions, on the need to report/notify the cyber-attacks.
4. develops the national framework for public awareness in cooperation with the public, private and academic stakeholders to ensure an effective approach on training the population on the behaviour, reaction, and cyber resilience in the online environment.
5. carries out and participates in prevention and awareness campaigns/actions on the root causes and consequences of cyber-attacks against the civilian networks at international, national, and regional level.

h) The function of cooperation and collaboration

1. ensures the cooperation framework to carry out specific cyber security activities, research, information exchange, training, education, awareness, project development, as well as any other activities necessary to ensure cyber security in Romania, according to legal competencies.
2. represents Romania in the established formats of international cooperation within its fields of competence, in cooperation with other state competent authorities, for ensuring inter-

institutional cooperation, mutual information and for maintaining a coherent position at international level.

3. supports national efforts, competent state institutions and authorities as well as the cooperation initiatives within the international organizations where Romania is involved - especially within the European Union (Uniunea Europeană) (EU/UE), the United Nations (Organizația Națiunilor Unite) (UN/ONU), the Organization for Security and Co-operation in Europe (Organizația pentru Securitate și Cooperare în Europa) (OSCE), and North Atlantic Treaty Organization (Organizația Tratatului Atlanticului de Nord) (NATO).
4. in collaboration with other competent authorities, universities, research centres, and economic operators, participates in the development of technological solutions for cyber security, with a dual use, civilian and military.
5. establishes, coordinates and manages the National Platform for Cyber Security Cooperation (Platforma Națională de Cooperare în Domeniul Securității Cibernetice), hereinafter referred to as NPCSC (PNCDSC), between state bodies, private sector, academia and non-governmental organizations, in order to ensure a unitary national framework of expertise, research, information and any other actions related to the field of competence.
6. participates in cooperation, working or specialized groups, and in cooperation networks, fora and organizations in the field of cyber security, as established at national, European, and international level.
7. develops partnerships with other national or international bodies with competencies and responsibilities in the field of cyber security, by concluding memoranda and protocols for cooperation with public or private law actors, whether national or foreign.
8. cooperates with the bodies from NDPONSS as well as from CSOC to ensure Romania's cyber security.
9. Cooperates with the Ministry of Research, Innovation and Digitalisation as well as the European Cybersecurity Industrial, Technological and Research Skills Centre for cyber security, in the fields of competence
10. Supports the participation of Romanian state bodies and of other stakeholders in national and international cyber security projects.

i) **The function of national cyber security certification authority** – as national competent body, ensures the national mechanisms regarding the evaluation, certification, and accreditation of cyber security products, services, and processes.

1. NCSD is the national cyber security certification authority for the civilian cyberspace. In this capacity, it certifies the cyber security aspects of the cyber security technology, products and services.
2. establishes norms, technical requirements, standards and procedures for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Cybersecurity Agency) and on cyber security certification for information and communication technology and repealing Regulation (EU) No 526/2013 (the Cyber Security Regulation).
3. sets up and manages the National Register of Cyber Security Assets, Products and Services (Registrul Național al Activelor, Produselor și Serviciilor de Securitate Cibernetică), hereinafter referred to as NRCSAPS (RNAPSSC). The methodological norms for the organisation and functioning of the register shall be approved within 120 days from the date of entry into force of this ordinance, by order of the DNSC Director which shall be published in the Official Gazette of Romania, Part I.
4. authorises civilian laboratories for testing, evaluating and certifying the cyber security of products and services used in the computer networks and information systems.

5. cooperates with national and international institutions in the field of standardization and accreditation of the products, services, and processes in the field of cyber security.

j) The function of ensuring compliance and unitary approach to cyber security within cyber infrastructures - issues opinions on the compliance of projects involving information systems and networks, other than those to be implemented in the infrastructures of the NDPONSS institutions, against the technical requirements and norms in the field of cyber security as required at national and international level.

1. endorses from the point of view of cybersecurity projects financed by public funds or for which government guarantees have been requested involving networks and IT systems covered by Law 362/2018. The approval shall be carried out by reference to the technical requirements and norms in the field of cybersecurity adopted at national and international level.
2. verifies and validates compliance of the implementation of cyber security measures in the projects referred to in point 1.
3. the rules on approval, verification and validation from the point of view of cybersecurity referred to in items 1 and 2 shall be approved within 180 days of the entry into force of this emergency ordinance, at the proposal of the DNSC Director, by order of the Secretary General of the Government, which shall be published in the Official Gazette of Romania, Part I.

k) **Representation function -** performs, on behalf of Romania, the representation role in the national, regional, European, and international bodies and organizations, acting as a national authority for its field of activity, in accordance with the applicable law.

l) Research and development function

1. consolidates, supports, and promotes the national potential for research, development, and innovation of the top cyber security activities, processes, and technologies, based on the individual and collective capacities of public and private sector, of the academic environment and industry.
2. carries out and participates in research and development activities in the field of cyber security and drafts procedures and recommendations regarding cyber security, according to the legal provisions regarding scientifical research and technological development.
3. develops studies and research on the issue of security of cyber products, services, and infrastructures.
4. develops and updates methodological, procedural, and good practice framework on scientific research activity in the field of cyber security, by consulting with institutions that have responsibilities and competencies in the field.
5. plans and carries out scientific research activities in its fields of competence, by cooperating at central and local level with public, private and academic stakeholders, as well as with natural persons.
6. develops relationships on scientific research with universities, research institutes, publishing houses, libraries, and specialists from Romania and abroad.
7. promotes scientific initiative, development, and innovation in specific cyber security areas in order to support and protect national interests in this field.

m) **Analysis and forecasting function** - evaluates and analyses the developments in the field of cyber security and issues alerts, analyses, newsletters and forecast bulletins.

n) The function of identification, evaluation, monitoring and mitigation of cyber risks at national level.

o) The function of national centre for managing cyber crises in peacetime

1. within the NCSD, it is established the National Centre for Cyber Security Crisis Management (Centrul Național de Gestionare a Crizelor de Securitate Cibernetică), hereinafter referred to as

NCCSCM (CNGCSC), which includes representatives of competent institutions and authorities, with responsibilities in the field of cyber security.

2. together with the institutions of NDPONSS, NCCSCM ensures the processing and analysis of data and information regarding cyber-attacks targeting the national space, with potentially major impact on the networks and information systems, done throughout analytical products, aimed to support the strategic level decision or to operationally support for cyber crisis management.

3. through collaboration with the other permanent members of CSOC, NCCSCM ensures the management of cyber crises caused by cyber-attacks, in collaboration with state bodies that have competencies and responsibilities for managing crises with impact on the proper functioning of the state.

p) The function of cyber security assessment of new technologies

1. evaluates from the point of view of cyber security the industrial control systems, computer systems and complex networks, products and services, as well as other new technologies.

2. identifies cyber security vulnerabilities and their impact on cyber security of Romania.

q) Evaluation and certification function

1. evaluates, tests, and certifies cyber security products and services, for its own needs or at the request of NDPONSS institutions and/or the Government.

2. establishes rules, prescriptions, or specifications for cyber security activities or for their results in order to ensure a unitary approach at national level, for achieving a high level of cyber security.

3. in collaboration with specialized bodies participates in the development approval and adoption of standards in its field of competence and makes them publicly available.

4. participates in national and international technical committees for the implementation of accepted technical standards and specifications, applicable to security of networks and information systems, without imposing or discriminating in favour of a certain type of technology.

r) The function of education and training in the field of cyber security

1. develops partnerships with ministries, schools, high schools/colleges, and universities, with private sector, as well as with international partners, to create the national framework for cyber security education and training to further provide the necessary human resources for ensuring the cyber security of Romania.

2. promotes the education and professional training of students with regards to cyber security, to ensure the implementation and use of new technologies daily.

3. carries out actions, exercises and seminars for preparation and training.

4. initiates and coordinates, in collaboration with representatives of the public, private and academic stakeholders, the establishment and development of central and regional centres cyber security of excellence, with the aim of preparing qualified human resources for national needs, conducting cyber security research and development activities, as well as any other activities necessary to ensure a high level of cyber security in Romania. These activities may include but are not limited to training of the human resources of other states.

5. upon request, certifies the centres of excellence, and education and training programs in the field of cyber security.

s) **The management function of projects and services for activities** is performed without prejudice to the activities foreseen in art. 5 letter b) and letter q) as follows:

1. NCSD leads, executes and participates in the identification, coordination, and implementation of projects of mutual interest, with internal and external financing both on its own account and

in partnership and facilitates the access of institutions, economic operators and persons authorised to these projects.

2. during the implementation of the project-specific activities referred to in paragraph 1, NCSD may create or participate in structures without legal personality, departments, departments, laboratories or other legal or organisational structures necessary to achieve its objectives, functions and duties, in compliance with the applicable law.

Art. 6 Management

(1) The NCSD management is ensured by the Director of NCSD and five deputies of the Director of NCSD, who have the rank of state secretary, respectively undersecretaries of state.

(2) The Director of NCSD and the five deputies of the Director of NCSD are appointed and released from office by decision of the Prime Minister, based upon an opinion issued by the SCND.

(3) The regime of incompatibilities and conflict of interests applicable to the Secretary of State and Undersecretary of State, as mentioned by Book I, Title IV of Law no. 161/2003 with regards to some measures for ensuring transparency in the exercise of public responsibilities, public office and in business environment, and for prevention and penalise corruption, with subsequent amendments and completions, are applicable to the Director of NCSD and to the five deputies of the Director of NCSD.

(4) The length of the mandate of the Director of NCSD is of 5 years, with the possibility of extension only once, for not more than 5 years.

(5) The mandate of the Director of NCSD ends in the following circumstances:

a) in case of impossibility to fulfil her/his mandate for more than 120 consecutive calendar days out of a period of 140 days;

b) in case of criminal conviction by final court decision, for which the rehabilitation did not intervene;

c) in case of withdrawal of the opinion issued by the SCND;

d) by resignation;

e) by death;

f) at the expiration of the term of the mandate.

(6) If the position of the Director of NCSD becomes vacant, under the conditions of para. (5) letters a) - e) a new person is appointed for this position for the remaining term of office, under the conditions of the provisions of paragraph (3).

(7) In case of vacancy of the position of the Director of NCSD, until the designation and appointment, in accordance with the law, of a new Director, for the remaining term of office, the interim shall be ensured by one of the Deputy Directors.

Art. 7 Representation

(1) The Director of NCSD represents the institution in relation with other public authorities and institutions, non-governmental organizations, as well as any legal or natural persons from Romania or from abroad.

(2) The Director of NCSD is the tertiary credit officer in accordance with the law.

(3) In her/his duties, the Director of NCSD can issue decisions and orders.

(4) The normative decisions and orders are published in the Official Gazette of Romania, Part I.

(5) The decisions and orders issued while performing the duties established by law, including those adopted in accordance with the provisions of Law no. 362/2018, can be challenged in administrative litigation, in accordance with the law.

(6) NCSD communicates to the European Commission information regarding the implementation of the European normative acts that fall within the fields of competence of the institution, based on the established deadlines or at the specific request of the European Commission.

Art. 8 Roles and responsibilities of the NCSD management

(1) The Director of NCSD has the following main duties:

a) Submits for Prime Minister's approval, based on the opinion issued by the SCND, the institutional development strategy of the NCSD, the activity and cooperation programs and the annual activity plan of the NCSD.

b) Approves the investment plans of NCSD.

c) Convenes and chairs the meetings of the Board of Directors of NCSD.

d) Sets up the location of the regional and county structures of NCSD, structures without legal personality.

e) Sets up by internal decision the specific roles and responsibilities of each functional compartment within NCSD.

f) Approves the internal regulations of NCSD.

g) Approves, in accordance with the law, the employment, promotion, as well as the modification or termination of the employment contracts of the NCSD staff.

h) Presents to SCND the activity report of NCSD, on annual basis.

i) Submits for approval by SCND, the documents concerning NCSD governance, respectively the staffing schedule, organizational structure and the internal regulations concerning governance and operations as well as any modification thereof.

(2) The Director of NCSD can delegate to her/his deputies the duties listed in paragraph (1).

(3) In the absence of the Director of NCSD, her/his duties are fulfilled by that deputy of the Director of NCSD appointed for this by decision of the Director of NCSD.

(4) If both the Director of NCSD and the deputies of the Director of NCSD are absent or temporarily unable to exercise their duties, the NCSD representation is ensured by a person with a management position appointed for this by decision of the Director of NCSD.

Art. 9 Board of Directors

(1) In its activity, the NCSD management is supported by the NCSD's Board of Directors, which operates based on a statute drafted by NCSD that is approved by the Prime Minister, based on the opinion issued by the SCND.

(2) The Board of Directors consists of representatives of:

a) The Presidential Administration;

b) The Prime Minister;

c) The Ministry of Internal Affairs;

d) The Ministry of National Defence;

e) The Ministry of Foreign Affairs;

f) The Ministry of Finances;

g) The Ministry of Labour and Social Protection;

h) The Ministry of Research, Inovation and Digitalisation;

i) The Ministry of Education

j) The Romanian Intelligence Service;

k) The Foreign Intelligence Service;

l) The Special Telecommunications Service;

m) The Protection and Guard Service;

n) The National Authority for Management and Regulation in Communications;

o) The National Registry Office for Classified Information.

(3) The members of the Board of Directors are appointed by the management of the institutions mentioned in paragraph (2).

(4) The Director of NCSD and the deputies of the Director of NCSD are members of the Board of Directors.

(5) The Board of Directors has the following duties and competencies:

a) Endorses the development strategies of NCSD and public policy proposals drafted by NCSD, aimed to prevent and counteract incidents within the cyber infrastructures.

b) Endorses the draft annual budget, the annual activity plan, and the annual activity report of NCSD.

c) Follows the development in conditions of economic efficiency and professional performance of the NCSD's activity.

d) Formulates recommendations regarding the objectives of the annual activity plan of NCSD.

e) Formulates recommendations on national points of view that must be supported by the NCSD representatives in the international cooperation context.

f) Analyses NCSD's activity based on the activity reports presented by the Director of NCSD.

g) Issues opinions on the documents concerning NCSD governance, as well as any modification thereof, respectively the staffing schedule, organizational structure and the internal regulations concerning governance and operations.

h) Supports the NCSD management in fulfilling the institutional objectives assumed by this act and by the internal regulations concerning governance and operations.

(6) The Board of Directors carries out its activity in quarterly meetings, in ordinary meetings, or whenever necessary, in extraordinary meetings.

(7) When exercising its attributions, the Board of Directors issues opinions and recommendations, which are adopted with the vote of the simple majority of its members present at the meeting.

(8) The Secretary's Office of the Board of Directors is performed by NCSD.

Art. 10 Regulatory Committee

(1) The Regulatory Committee is established as guarantor of the objectivity, transparency, neutrality, equidistance, non-discrimination, and legality of the regulatory activities carried out by NCSD, providing for this purpose specialized support, through guidelines and recommendations on ensuring compliance with the principles of objectivity, transparency, neutrality, equidistance, non-discrimination, and legality in the regulatory activity of NCSD.

(2) The Regulatory Committee has an advisory role and consists of:

a) three members from NCSD, appointed by decision of the Director of NCSD.

b) one member from each of the institutions mentioned in art. 9 paragraph (2).

(3) The appointment and revocation of the members of the Regulatory Committee is made by the Board of Directors based on the proposal by the institutions mentioned in paragraph (2).

(4) One of the NCSD members appointed in accordance with paragraph (2) item a) shall convene and chair the meetings of the Regulatory Committee..

(5) Members of the Regulatory Committee must meet the following requirements:

a) must be Romanian citizens, with a permanent residence in Romania, with a good ethical and professional reputation, attested by the nominee institutions by letter of recommendation.

b) must be higher education graduates and must have a background in the technical, economic, or legal field, with at least 10 years of work experience.

c) must have a minimum experience of 5 years in management positions in the field of cyber security, networks, and information systems or in the NDPONSS.

(6) The Regulatory Committee members have a 3 year term of office.

(7) In case of impossibility of exercising the mandate by one of the members, the institutions mentioned in paragraph (2) designate a new person under the conditions of paragraph (3) and (5) for the remaining term of office.

(8) It is considered impossibility to exercise the mandate, any circumstance that creates unavailability with a duration of more than 90 consecutive days.

(9) The activity of the Regulatory Committee is carried out based on the statute of the Regulatory Committee, elaborated by NCSD and based upon an opinion issued by SCND.

(10) The Secretary's Office of the Regulatory Committee is provided by NCSD through the functional department that manages the regulatory activity.

Art. 11 Financing

(1) The financing of the current and capital expenses of NCSD is done entirely from the state budget, through the budget of the General Secretariat of the Government.

(2) NCSD sets and collects:

a) the amount of tariffs for services of the activities referred to in art. 22, paragraph (1), letter 1), art. 32 paragraph (2), letters c) and e) and art. 33, paragraph (2), letters c) and e) of Law no. 362/2018, established by decision of the Director of NCSD, which are published in the Official Gazette of Romania, Part I;

b) the amount of tariffs for registration in the National Register of Cyber Security Assets, Products and Services;

c) the amount of tariffs for the authorization of the civilian laboratories for testing, evaluation, and certification of the cyber security of the products and services that are used within the computer networks and systems;

d) the amount of tariffs for endorsement, verification and validation of compliance on cyber security;

e) the amount of tariffs for certification of the cyber security of the solutions, products and services of the information and communications technology, including the new technologies;

f) revenues from specialized services;

g) revenues from the provision of cyber security products and services;

h) royalties from intellectual property rights and licenses;

i) commissions for partnerships and projects;

j) other revenues established by government decision.

(3) The resources foreseen under paragraph (2) shall be made to the state budget. The amounts collected pursuant to paragraph (2) shall be transferred by the NCSD to the state budget within a maximum of 5 working days from their receipt..

Art. 12 Analysis of the NCSD activity

(1) The activity of NCSD is analysed by SCND based on the annual report, which is presented for the previous year, as well as on the specific reports drawn up at the request of SCND.

(2) The annual activity report shall be submitted to the SCND, until March 31, after approval by the Board of Directors.

(3) NCSD drafts reports, analyses and alerts regarding the cyber security of the national cyberspace, of the national interest cyber infrastructures, of the networks and information systems from the fields of competence, which are presented towards the Prime Minister, the President, SCND, CSOC and towards the institutions with attributions within NDPONSS, as well as to the Board of Directors.

Art. 13 The NCSD staff

(1) The NCSD staff consists of own contractual staff or staff seconded from NDPONSS, employed according to NCSD's staffing schedule.

(2) The staffing schedule, organizational structure and the internal regulations concerning governance and operations of NCSD as well as any modification thereof shall be approved by the SCND. The staffing schedule also includes the positions filled-in by staff coming from NDPONSS.

(3) The maximum number of staff positions is 1250, including central, regional and county structures, excluding dignitaries and posts related to dignitaries' cabinets.

(4) In addition to the functions provided for in Framework Law No 153/2017 on the remuneration of staff paid from public funds, as amended and supplemented, the NCSD's staffing schedule contains specific management and execution functions as follows:

a) Management positions: Senior cyber security manager, Cyber security manager, Senior cyber security coordinator, Cyber security coordinator.

b) Execution positions (higher education): Expert in cyber security, Expert in data collection, primary analysis and cyber security incident response, Expert in digital investigations and malware analysis, Expert in development, implementation and management of cyber security infrastructures, Expert in open source analysis, cyber security risks and threats, Expert in funding, implementation and administration of cyber security projects, Expert in legal policies and cyber security standardization, Expert in cyber security evaluation and financial impact assessment, Expert in cyber security policies, strategies and cooperation, Expert in development of cyber security capabilities, skills and knowledge.

c) Execution positions (secondary education): Assistant in cyber security, Assistant in data collection, primary analysis and cyber security incident response, Assistant in digital investigations and malware analysis, Assistant in development, implementation and management of cyber security infrastructures, Assistant in open source analysis, cyber security risks and threats, Assistant in funding, implementation and administration of cyber security projects, Assistant in legal policies and cyber security standardization, Assistant in cyber security evaluation and financial impact assessment, Assistant in cyber security policies, strategies and cooperation, Assistant in development of cyber security capabilities, skills and knowledge.

Art. 14 Staff employment and promotion

The NCSD staff is employed based on a competition or examination organized in accordance with the law, based on the organizational structure, and the specific management and execution functions within the DNSC shall be established in accordance with Article 28 of the Framework Law no. 153/2017, as amended and supplemented, by assimilating with the basic functions and salaries set out in the annexes to the Framework Law and applicable to the category of personnel concerned, with the opinion of the Ministry of Labour and Social Protection and of the Ministry of Finance, within 45 days from the date of entry into force of this emergency ordinance..

Art. 15 Patrimony

(1) On the date of entry into force of this Emergency Ordinance, the NCSD shall take over the assets, archives and committed budget appropriations, including for the entire current year, within the limits of the commitment appropriations and for the purposes for which they were approved to the National Cyber Security Incident Response Centre - CERT-RO, which shall be disbanded.

(2) NCSD undertakes all rights and obligations of CERT-RO, including those coming from the litigations pending before the courts and acquires his legal standing.

(3) The handover of the patrimony is performed based on the financial statements prepared according to the provisions of art. 28 paragraph (1A1) of the Accounting Law no. 82/1991, republished, with the subsequent amendments and completions and of the handover drawn up within 30 days from the date of closing the CERT-RO. The handover protocol shall also cover budget appropriations, commitment appropriations and budget implementation for the current year.

Art. 16 Cooperation

(1) NCSD cooperates with international organizations and bodies in its fields of competence.

(2) NCSD represents Romania at the level of the European Union institutions and at the level of other international forums in its fields of competence.

(3) To ensure an adequate capacity for identification, evaluation, and adoption of risk management measures and/or response to cyber incidents and attacks, NCSD develops information exchange and transfer of expertise with other institutions and authorities with responsibilities in the field, it promotes and supports cooperation between public and private sectors, as well as cooperation with non-governmental media and academic community.

(4) NCSD may be a contributing member in national and international organizations and bodies, in its fields of competence.

Art. 17 Roles and responsibilities in situations of cyber crisis in peacetime

(1) The specific roles and responsibilities, governance and operations of the NCCCM are established by the internal regulations concerning governance and operations of the NCCCM, which is developed by NCSD within 180 days from the entry into force of this Emergency Ordinance and it is approved by the Director of NCSD, after consulting the other permanent members of the CSOC.

(2) The NCSD management shall issue the necessary measures to ensure the operational capacity of the institution, including of the NCCCM for the management of the cyber crisis in peacetime.

Art. 18 Authorization of civilian laboratories

(1) In the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council of April 17, 2019 on ENISA (the European Union Agency for Cyber Security) and on the certification of cyber security for information and communication technology and repealing Regulation (EU) no. 526/2013 (Regulation on cyber security), the cyber security products and services used in computer networks and systems are tested, evaluated and certified by economic operators that have the quality of authorised civilian laboratories. The functioning of the authorised civilian laboratories that carry out activities of testing, evaluation, and certification of the cyber security of the products and services that are used within the networks and computer systems, is subject to prior authorization from NCSD

(2) Granting, extension, suspension, or withdrawal of the authorization mentioned in the paragraph (1) shall be performed based on the rules for authorization and verification of the civilian laboratories for testing, evaluation, and certification of cyber security of products and services that are used in computer networks and systems, as developed by NCSD and as approved by Government's decision. The authorization is valid for a maximum of 3 years.

(3) The request for authorising the civilian laboratories mentioned in paragraph (1) accompanied by the documentation set by the regulation mentioned in paragraph (2) shall be transmitted to the NCSD in physical format or by electronic means.

(4) Within 10 days from the receipt of the applicant's request, NCSD informs if the documentation is complete or requests additional relevant information.

(5) Within maximum of 60 days from the date of receipt of all requested information, NCSD issues the authorization of laboratory for testing, evaluation, and certification of cyber security of products and services that are used in computer networks and systems, or informs the applicant on its negative decision.

(6) NCSD duly justifies any decision by which it denies the authorization of laboratory for testing, evaluation, and certification of cyber security of products and services that are used in computer networks and system.

(7) The civilian laboratories referred to in paragraph 1 shall be (1) shall be subject to control by the NCSD in order to determine the degree of compliance with their obligations under this Emergency Ordinance.

Art. 19 Control activity of civilian laboratories

(1) NCSD exercises the control of the activity carried out by the civilian laboratories for testing, evaluation, and certification of the cyber security of the products and services that are used within the computer networks and systems.

(2) The control of the fulfilment of the obligations by the civilian laboratories is carried out based on the rules of authorization and control of the civilian laboratories mentioned at art. 18 paragraph (2).

(3) The following acts represent violations if they were not committed in such conditions as to be considered crimes according to the law:

a) the use of the title of approved civilian laboratory without an authorisation granted by the NCSD pursuant to art. 18 paragraph (1);

b) the provision of test, evaluation or certification reports or certificates by unauthorised civilian laboratories or without a valid authorisation pursuant to art. 18 paragraph (1);

c) the refusal of the civilian laboratory to submit to the control initiated by NCSD according to art. 18 paragraph (7).

(4) By derogation from the provisions of art. 8 paragraph (2) letter a) of Government Ordinance no. 2/2001 regarding the legal regime of violations approved with modifications and completions by Law no. 180/2002, with the subsequent amendments and completions, violations mentioned in paragraph (3) are sanctioned as follows:

a) with a fine from 5,000 lei to 50,000 lei and in case of committing a new violation within 6 months, from the date of committing the first violation, the maximum limit of the fine is 200,000 lei;

b) for the economic operators with a turnover above 1,000,000 lei, with a fine in the amount of up to 5% of the net turnover, and in case of committing a new violation within 6 months from the date of committing the first violation the maximum limit of the fine is 10% of the net turnover.

(5) The net turnover mentioned in paragraph (4) letter b) is the one reported in the last annual financial statements.

(6) In order to determine the penalty referred to in paragraph 4, the NCSD shall take into account the degree of concrete social danger of the offence and the period of time during which the legal obligation was breached. For authorised natural persons,

(7) For the authorised natural persons, sole proprietorships and family businesses, the turnover referred to in paragraph (4) letter b) shall correspond to the total income of those economic operators in the financial year preceding the sanction.

(8) For the newly established entities and for the entities that did not register yet the turnover in the year prior to the sanction, the fine mentioned in paragraph (4) shall be established to the amount of a minimum of one and a maximum of 25 minimum gross salaries per economy.

(9) To the extent that this Emergency Ordinance does not mention otherwise, for the violations mentioned in the paragraph (3) the provisions of the Government Ordinance no. 2/2001 regarding the legal regime of violations, approved with modifications and completions by Law no. 180/2002, with the subsequent modifications and completions, shall be applied.

(10) Establishing the violations mentioned in paragraph (3) shall be performed by the control personnel of NCSD and the enforcement of the corresponding sanction is by decision of the Director of NCSD.

(11) The decision mentioned in the paragraph (9) must include the following: the identification data of the offender, the date, the description of the violation and the circumstances considered, indicating the legal basis according to which the violation is established, the sanction applied, the term and the manner of payment of the fine, the term of exercising the appeal and the competent court.

(12) If necessary, the Director of DNSC shall refer to the Competition Council the existence of possible anti-competitive acts or facts.

(13) By derogation from the provisions of art. 13 of the Government Ordinance no. 2/2001, approved with modifications and completions by Law no. 180/2002, with subsequent modifications and completions, the sanction according to paragraph (4) has a statute of limitation of one year from the date of committing the fact. In case of violations that last in time or those consisting in committing, based on the same resolution, at different time intervals, several actions, or inactions, which each have the content of the same violation, the statute of limitation begins from the date the finding or from the date of cessation of the last act or fact committed, if this moment occurs prior to the finding.

(14) By way of derogation from the provisions of Article 14 paragraph (1), of Government Ordinance No 2/2001, approved with amendments and additions by Law No 180/2002 with subsequent amendments and additions, the decision referred to in paragraph (10) shall be communicated to the offender within 15 days from the date of issue of the decision.

(15) Together with the decision mentioned in paragraph (10), the offender is also notified of the payment notice, which contains the mention regarding the obligation to pay the fine within 30 days from the date of communication of the decision.

(16) The decision mentioned in paragraph (10) is an enforceable title, without any other additional formality. The action in administrative contentious under the conditions of paragraph (18) adjourns the execution only in terms of payment of the fine, until the court pronounces a final decision.

(17) The amounts resulting from the fines applied in accordance with the provisions of this article represent revenue to the state budget. Enforcement is carried out in accordance with the legal provisions regarding the foreclosure of fiscal receivables. To enforce the sanction, NCSD communicates ex officio to the specialized bodies of the National Agency for Fiscal Administration (Agenția Națională de Administrare Fiscală) the decision mentioned in paragraph (10), after the expiration of the term mentioned in the payment notice or after the finality of the court decision by which the action was settled in administrative litigation.

(18) By derogation from the provisions of art. 7 of the Law on administrative litigation no. 554/2004, with the subsequent amendments and completions and from the provisions of art. 32 paragraph (1) of Government Ordinance 2/2001 approved with amendments and additions by Law No 180/2002 with subsequent amendments and additions, the decisions adopted according to this Emergency Ordinance may be challenged in administrative contentious at the Bucharest Court of Appeal, without going through the preliminary procedure, within 30 days from their communication.

(19) In the exercise of the attributions mentioned in art. 5 letter i) NCSD notifies the Competition Council (Consiliul Concurenţei) regarding the existence of possible anti-competitive facts or acts.

(20) The provisions of art. 19 shall enter into force within 30 days from the date of the publication of this emergency Ordinance.

Art. 20 Final and transitional provisions

(1) This Emergency Ordinance does not apply to the areas of activity under the responsibility of the institutions of defence, public order and national security, national critical infrastructures and infrastructures that uses classified information.

(2) The list of state-owned assets that are public property, as well as the list of state-owned assets that are private property, taken over in administration by NCSD, shall be approved by decision of the Government, within 30 days from the date of entry into force of this Emergency Ordinance.

(3) Re-employment of the staff taken over according to article 1 paragraph (3) in the organizational structure of NCSD is carried out within the terms and with the procedure provided by law.

(4) From the date of approval by the SCND of the staffing schedule, the organizational chart and the internal regulations concerning governance and operations of NCSD, shall start the procedure for filling the vacancies in the new organizational structure, enshrined in the approved annual budgetary provisions.

(5) Within 180 days from the date of entry into force of the Emergency Ordinance hereby, the rules for authorization and verification of the civilian laboratories for testing, evaluation, and certification of the cyber security of products and services used in computer networks and systems shall be approved by Government's decision.

(6) The methodological rules for the organization and functioning of the register referred to in Article 5 letter i) item 3 shall be approved within 120 days from the date of entry into force of this Ordinance, by order of the Director of the DNSC to be published in the Official Gazette of Romania, Part I.

(7) The rules on the modalities of endorsement, verification and validation in terms of cyber security provided for in Article 5 (j) (1) and (2) shall be approved within 180 days of the entry into force of this Emergency Ordinance, at the proposal of the Director of the DNSC, by order of the Secretary General of the Government, which shall be published in the Official Gazette of Romania, Part I.

(8) By derogation from the provisions of art. 27 paragraph (3) of Law no. 55/2020 regarding some measures for preventing and combating the effects of the COVID-19 pandemic, with the subsequent modifications and completions, during the alert state, contests, or examinations for filling vacant or temporarily vacant positions in the organizational structure of NCSD may also take place.

(9) Throughout the Law no. 362/2018 on ensuring a high common level of security of computer networks and systems, published in the Official Gazette of Romania, Part I, no. 21 of January 9, 2019, with subsequent amendments and completions, the phrases "National Cyber Security Incident Response Team - CERT-RO" and "General Secretary's Office of the Government" shall be replaced by the phrase "National Cyber Security Directorate", the phrase "CERT-RO" with the phrase "NCSD", and the phrase "General Secretary of the Government" with the phrase "Director of NCSD".

(10) On the date of entry into force of this emergency ordinance, the Government Decision no. 494/2011 on establishing of the National Cyber Security Incident Response Team - CERT-RO, published in the Official Gazette of Romania, Part I, no. 388 of June 2, 2011, with subsequent amendments and completions is repealed.

PRIME-MINISTER

FLORIN-VASILE CÎȚU

Bucharest, 22 September 2021.

No. 104.

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

LAW 11/2022

for the approval of Government Emergency Ordinance 104/2021 on establishing the National Cyber Security Directorate

The Romanian Parliament adopts the hereby law.

Single article – The Government Emergency Ordinance No. 104 of 22 September 2021 on the establishment of the National Cyber Security Directorate, published in the Official Gazette of Romania, Part I, No. 918 of 24 September 2021, is hereby approved, with the following amendments and additions:

1. Article 1, paragraph (6) is amended, and it will read as follows:

"(6) The NCSD shall have responsibilities for cyber security of the national civil cyberspace, a component of the national security."

2. Article 5, letter b), point 5 is amended and it will read as follows:

"5. performs the tasks of the competent national cybersecurity authority for hosting service providers, cloud service providers and content distribution network providers;".

3. Article 20, a new paragraph (8^{1}) is inserted after paragraph (8), with the following content:

"(8^{1}) By way of derogation from the provisions of Article 16 paragraph 1) of the Framework Law no. 153/2017 on the salaries of staff paid from public funds, as amended and supplemented, the staff nominated in the teams of projects financed from European or international programmes, instruments, mechanisms or funds in which NCSD participates shall be paid at the hourly/daily/monthly rate specified in the funding contract. If the funding contract does not specify the hourly/daily/monthly rate, the ceilings specified in the National Plan for Research - Development and Innovation in force shall be used."

The hereby law was adopted by the Romanian Parliament, in compliance with the provisions of Art. 75 and Art. 76 paragraph (1) of the Romanian Constitution, republished.

PRESIDENT OF THE CHAMBER OF DEPUTIES
ION-MARCEL CIOLACU

On behalf of the PRESIDENT OF THE SENATE,
ROBERT-MARIUS CAZANCIUC

Bucharest, 7 January 2022

No. 11

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

DECREE 27/2022

on the promulgation of the Law approving the Government Emergency Ordinance 104/2021 on establishing the National Cyber Security Directorate

Pursuant to the provisions of Article 77 paragraph (1) and article 100 paragraph (1) of the Romanian Constitution, republished,

The President of Romania hereby decrees:

Single article – The Law approving the Government Emergency Ordinance No. 104/2021 on establishing the National Security Directorate is passed and the publication of this law in the Official Gazette of Romania, Part I, is hereby ordered.

PRESIDENT OF ROMANIA

KLAUS-WERNER IOHANNIS

Bucharest, 7 January 2022.

No. 27.